IN THE DISTRICT COURT OF THE UNITED STATES
FOR THE DISTRICT OF SOUTH CAROLINA
FLORENCE DIVISION

UNITED STATES OF AMERICA, Plaintiff, vs. $593,345 in U.S. Currency; $99,258 in U.S. Currency; and $41,195 in U.S. Currency, Defendant *in Rem*.	)	CIVIL ACTION NO.: 4:24-cv-5783-JD

UNITED STATES' COMPLAINT FOR FORFEITURE *IN REM*

The Plaintiff, United States of America, brings this complaint and alleges as follows, in accordance with Rule G(2) of the Supplemental Rules for Admiralty and Maritime Claims and Asset Forfeiture Actions.

NATURE OF THE ACTION

1. This is a civil action *in rem* to forfeit to the United States of America funds in the amount of $593,345 in U.S. Currency; $99,258 in U.S. Currency; and $41,195 in U.S. Currency ("Defendant Funds"), pursuant to 18 U.S.C. § 981(a)(1)(A) and 18 U.S.C. § 981(a)(1)(C). The United States seeks forfeiture based upon a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitute, or are traceable to:

a. property involved in wire fraud transactions, attempted wire fraud transactions, or conspiracy of same in violation of 18 U.S.C. §§ 1343, 1349;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i), and/or § 1956(a)(2);

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960;

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7);

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h); and

f. property involved in money transactions in criminally derived property or attempted money transactions, in violation of 18 U.S.C. § 1957.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over an action commenced by the United States pursuant to 28 U.S.C. § 1345, and over an action for forfeiture by virtue of 28 U.S.C. § 1355. This Court has *in rem* jurisdiction over the Defendant Funds pursuant to:

(a) 28 U.S.C. § 1355(b)(1)(A), because acts or omissions giving rise to the forfeiture occurred in the District of South Carolina; and

(b) 28 U.S.C. § 1355(b)(1)(B), because venue properly lies in this district pursuant to 28 U.S.C. § 1395.

THE DEFENDANT *IN REM*

3. The Defendant Funds consist of $593,345 in U.S. Currency; $99,258 in U.S. Currency; and $41,195 in U.S. Currency obtained by agents with the Federal Bureau of Investigations (FBI) during an investigation into a transnational criminal organization involving cryptocurrency brokers who provide professional laundering services to the Hector PAEZ Garcias and David BENGAULT Jimenez money laundering organization. The Defendant Funds were seized from three bank accounts: $593,345 from Bank of America account ending in 4173 for "Rogas Management LLC"; $41,195 from Mercury Technologies account ending in 3543 for "Bereshit Royalty LLC"; and $99,258 from Bank of America account ending in 1398 for "Digital Design and Graphics LLC."

4. The FBI seized the Defendant Funds for federal forfeiture. The Defendant Funds are currently restrained and pending deposit to an account under the control of the FBI.

5. In accordance with the provisions of 19 U.S.C. § 1606, the Defendant Funds have a total domestic value of approximately $593,345 in U.S. Currency; $99,258 in U.S. Currency; and $41,195 in U.S. Currency.

KNOWN POTENTIAL CLAIMANTS

6. The known individuals whose interests may be affected by this litigation are:

   a. Jorge Carmona contacted the FBI regarding the seizure of the Defendant Funds and also had signatory authority over the Mercury Technologies account from which a portion of the Defendant Funds were seized.

b. Jose Redondo Jimenez has sole signatory authority over one account from which the Defendant Funds were seized.

c. Hugo Solano is owner of Digital Design and Graphics LLP, which maintained a bank account from which a portion of the Defendant Funds were seized.

d. Savannah Solano has signatory authority over the Digital Design and Graphics LLP account from which a portion of the Defendant Funds were seized.

BASIS FOR FORFEITURE

Pursuant to the pleading requirements of Supplemental Rule G(2)(f), Plaintiff alleges that there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds are subject to forfeiture to the United States, based in part upon the following:

1. The FBI is targeting a network of Central and South American-based cryptocurrency brokers who provided professional laundering services to the Hector PAEZ Garcia and David BENGUIAT Jimenez money laundering organization. Investigators developed specific evidence that the MLO has laundered more than $52 million in illicit drug trafficking proceeds between 2021 and 2023. The MLO laundered these trafficking proceeds for the benefit of major Mexican drug cartels, specifically traffickers associated with the Sinaloa Cartel.

2. PAEZ was indicted in 2023.

3. S1 is a foreign national from Costa Rica, who provided cryptocurrency laundering services to the MLO in 2022 and 2023. Most notably, S1 helped covert bulk cash proceeds to cryptocurrency, and transfer the cryptocurrency to Mexico. Like other MLO partners, S1's laundering activity is not limited to supporting the MLO. In May 2024, Jorge CARMONA Madrigal, a Costa Rica-based lawyer, worked with S1 to convert $935,500 into USDT and transfer

the funds to Costa Rica.[1] As detailed below, CARMONA and the fraud organization had the fraud victims wire money to the subject accounts from which the Defendant Funds were seized. S1 then converted a portion of the funds to USDT for transfer to Costa Rica.

4. Agents traced the seized funds and discovered that they had been wired by Victim 1, a middle-aged fraud victim residing in Maryland. The FBI also found an additional victim in the scheme, V2, an elder fraud victim residing in Missouri. V2 had been directed by fraudsters to deposit funds to the Subject Accounts.

5. As referenced in this Complaint, the Subject Accounts from which the Defendant Funds derived are described below:

- **Subject Account 1**: the records show that Jose REDONDO Jimenez opened Bank of America account 8981 3708 0215 and had sole signatory authority over the account. REDONDO represented that the account was to be used by the business "Rogas Management LLC."
- **Subject Account 2**: the records show that Jorge CARMONA Madrigal opened Mercury Technologies business account 2023 3886 3543. CARMONA represented that the account was to be used by the business "Bereshit Royalty LLC."
- **Subject Account 3**: the records show that Savannah SOLANO opened Bank of America account 2230 3210 1398 for "Digital Design and Graphics LLP" and had sole signatory authority over the account.

CHS Provides Reporting on Attempts by CARMONA to Launder Funds

6. In May 2024, a confidential human source reported that a Costa Rican attorney, CARMONA, was seeking to purchase large amounts of USDT. Among others, investigators learned, CARMONA was working with S1 to conduct this transaction.

[1] Tether (USDT) is what is known as a "Stablecoin" – a cryptocurrency designed to provide a stable price point at all times. The USDT cryptocurrency was created by Tether Limited to function as the internet's Digital Dollar, with each token worth $1.00 USD and allegedly backed by $1.00 USD in physical reserves.

7. On May 9, 20204, CARMONA arranged the transfer of $300,000 to a domestic account in the name of "Rogas Management" (*i.e.*, **Subject Account 1**). "Rogas Management LLC" purports to be a management and consultant company that caters to professional athletes. In fact, the business is a front for illicit cryptocurrency exchange services. Once the funds are transferred to the account, an equivalent amount of funds in USDT gets transferred to a virtual-currency wallet that S1 controls, in Costa Rica. Here, following the transfer of $300,000, an equivalent amount of USDT went to the wallet that S1 controls in Costa Rica.

8. On May 13, 2024, CARMONA deposited a cashier's check of $593,345 into **Subject Account 1**. He issued the check from his own domestic bank account at Wells Fargo, which was held in the name of "Carmona Inversiones LLC."

Investigators Trace the Origin of the Funds Sent by CARMONA

9. Law enforcement learned the following about a portion of the Defendant Funds

- May 8, 2024: CARMONA opened the account for "Carmona Inversiones LLC," with a $50 opening deposit. CARMONA was the sole signatory of the account.
- May 9, 2024: the "Carmona Inversiones LLC" account received an incoming wire transfer of $935,500 from the personal bank account for V1, at Farmers Bank of Willards.
- May 9, 2024: CARMONA transferred out a portion of the $935,500 via two wire transfers: $300,000 to the Bank of America account for "Rogas Management LLC" (**Subject Account 1**) and $42,100 to the Choice Financial (Mercury Technologies Inc.) bank account for "Bereshit Royalty LLC" (**Subject Account 2**).
- May 13, 2024: CARMONA used the remaining balance of his account to purchase a $593,345 cashier's check payable to "Rogas Management LLC."

Following the purchase of the cashier's check, the balance of CARMONA's account was $0.

Investigators Interview V1

10. The FBI identified V1 as the source of a portion of the Defendant Funds as the FBI had been investigating a fraud scheme targeting victims throughout the United States. An additional two victims of the fraud scheme reside in the Southern District of California. These victims, V3 and V4, have been repeatedly targeted by fraudsters in a lottery/sweepstakes scam.[2] V3 and V4 have sent over $500,000 to subjects working with the fraud ring between 2022 and 2024.

11. As part of the FBI's investigation, agents spoke with V1 several times and determined V1 had been victimized multiple times by the fraud ring. V1 was first victimized when the fraud ring convinced V1 that they had won a large amount of money in a sweepstakes. V1 sent large sums of money, at the direction of the fraudsters, which V1 believed were fees and taxes that had to be paid before V1 could receive the cash prize. The fraudsters continued to victimize V1 and even pretended to be federal law enforcement agencies.

12. V1 is a middle-aged mechanic residing in Maryland. V1 confirmed that he/she had sent a wire transfer in the amount of $935,500 to a company called "Carmona Inversiones." V1 stated that he/she was under a "federal gag order" and had done so at the direction of the "IRS." It is common for fraudsters to tell victims that they are under such "gag orders" to isolate the victims and prevent them from cooperating with legitimate law enforcement.

13. V1 said that he never intended the funds to be sent overseas, and that V1 never would invest, and never had invested, in cryptocurrency.

Bank of America Receives Fictitious Invoices Related to the CARMONA Transactions

14. On May 22, 2024, the FBI learned that Bank of America received a pair of invoices in an apparent attempt to explain the source of the funds sent by CARMONA. The first invoice

2 A "sweepstakes" or "lottery" scam is a common ploy utilized by fraudsters, especially to target the elderly. The scheme works as follows: fraudsters contact a victim and explain that they have won a large cash prize. However, before the prize can be disbursed, the victim must pay taxes and various other fees. The victim is repeatedly asked to pay different fees, but the "winnings" are never disbursed. These scams are typically located abroad and the funds paid by the victims are routed overseas, outside the reach of U.S. law enforcement.

was dated May 8, 2024, for the $300,000 deposit to **Subject Account 1**; the second invoice was dated May 13, 2024, for the $593,345 deposit to **Subject Account 1**. Both invoices showed that "Rogas Management LLC" provided a service in exchange for the deposits, in the form of "Sale of Technology Goods for Export." The payee was identified as "Carmona Inversiones LLC," and the listed point of contact was "JorgeCarmonaMadrigal4@gmail.com."

FBI San Diego Conducts Interview of CARMONA

15. The FBI provided its phone number to Bank of America to pass along to anyone inquiring about the status of the funds in **Subject Account 1.** Starting on May 23, CARMONA called me a dozen times before we returned his call. At the start of the call, CARMONA was advised that he was speaking to FBI Special Agents and that the call was recorded.

16. CARMONA confirmed his name and stated that he was the account holder for the Wells Fargo account "Carmona Inversiones." CARMONA explained that "Rogas Management" is a technology provider that also offers technology investments, and that the funds he had sent to **Subject Account 1** via the cashier's check (*i.e.*, the $593,345) was to pay them, apparently for these services.

17. During the call, CARMONA also said "Rogas Management" is a cryptocurrency provider. CARMONA then contradicted himself when he claimed the reason he sent the money to "Rogas Management" was to convert funds into cryptocurrency. CARMONA explained that he has clients who provide him funds that they want to invest by purchasing cryptocurrency such as Bitcoin. These clients are from a firm and there are "accountants" who recommend clients and know the client's name.

18. At this point of the interview, investigators informed CARMONA that the person who sent the $935,500 to his business account was the person with V1's name. CARMONA confirmed that V1 was the person who had sent him the $935,500 and said V1 was an investor who wanted to invest in cryptocurrency. Upon receiving the money, CARMONA wired the money to "Rogas Management." "Rogas Management," in turn, sent an equivalent amount of funds in

cryptocurrency to V1's wallet where he was located in "New York." CARMONA explained that he would receive a commission for completing the cryptocurrency investment on V1's behalf.

19. At the conclusion of the call, the interviewing agent asked CARMONA if he could provide invoices and documentation to support his statements about the origin and destination of the funds. CARMONA promised that he would send the requested documents. CARMONA subsequently sent several documents to FBI agents that attested to the origin of the funds. In summary these documents appear to be fictitious and appear to have been created in reaction to the funds being seized to portray the origin of the funds as legitimate. The representations made in the documents conflict with CARMONA's own statements. A number of inconsistences were noted:

- "Affidavit Source of Funds" – This document is signed by CARMONA and V1 and states that V1 instructed his bank to send $935,500 on "6/21/2024." This date is incorrect as V1 sent the funds on May 9, 2024.
- "Joint Venture Agreement" – This document attests that V1 and CARMONA are entering into a joint venture to "collaborate on digital marketing campaigns and investment opportunities to maximize profitability and market presence." V1 would provide an investment of $935,500 for the venture. The document is dated June 3, 2024 (several weeks after the funds were sent) and signed by V1 and CARMONA.
- "Invoices from Rogas Management" – These documents consist of two invoices issued by "Rogas Management" covering the $300,000 and $593,545 deposits. Both invoices state that the service provided by Rogas Management to CARMONA is "Sale of Technology Goods for Export."

Additional Details to Illustrate the Illicit Nature of the Transaction

20. Investigators identified additional facts further showing the illicit nature of the transaction. A review of CARMONA's travel records show that he traveled from Costa Rica to Orlando, Florida and spent nine days in the United States; during this time, he opened the "Carmona Inversiones" bank account and conducted all the transactions discussed herein.

CARMONA arrived in the United States on May 7, 2024, and on May 9, 2024, CARMONA opened the bank account for "Carmona Inversiones," an apparent investment business.

21. Open-source research on "Carmona Inversiones" (which translates to "Carmona Investments") found no evidence of the existence of the business other than the Florida incorporation documents associated with the entity. Searches for "Carmona Inversiones" and CARMONA within the registration databases of the Security and Exchange Commission and the Financial Industry Regulatory Authority (FINRA) were negative, showing that CARMONA is not a registered investment advisor, and his purported investment business is not a registered investment brokerage. The FBI's open-source research has identified a government of Costa Rica website indicating that CARMONA was employed as a public defender for the First Judicial Circuit of San Jose, Costa Rica.

22. The two addresses CARMONA provided for the location of the business are in fact townhouses in suburban neighborhoods in Florida.[3] There is no evidence for the existence of a business operating at those addresses. Prior to CARMONA's contact with the FBI, the FBI tried to call several phone numbers associated with "Carmona Inversiones" that were provided to Wells Fargo as points of contact for the business; all of the numbers were disconnected or not in service.

23. Immediately after opening the account, CARMONA received the $935,500 wire transfer from V1. That same day, CARMONA sent the first transfer of the funds ($300,000) to **Subject Account 1**, upon which the funds were exchanged for cryptocurrency that was transferred to Costa Rica. CARMONA also sent $42,100 to **Subject Account 2**. This amount is 4.5 percent of the $935,500 he received. This is a typical commission payment for someone in CARMONA's position when receiving and laundering illicit funds fraudulently obtained from victims like V1.

24. On May 13, 2024, CARMONA used the entire remaining balance of his "Carmona Inversiones" bank account to purchase the $593,345 cashier's check, which he deposited to

[3] CARMONA provided the address 2673 SE 12th Street, Homestead, FL as the location of the business in the Florida incorporation filing. CARMONA provided the address 13342 Abuela Aly, Windmere, FL as the location of the business when opening the bank account "Carmona Inversiones" at Wells Fargo.

Subject Account 1. Two days later, on May 15, travel records show that CARMONA left the United States and returned to Costa Rica.

25. This 1:1 transfer of funds through the "Carmona Inversiones" bank account is consistent with CARMONA operating a funnel account, described in detail below. Additionally, as noted by the Wells Fargo employee, there was no activity in the account other than rapid deposit and subsequent transfer activity. This is contrary to what one would expect for an investment business, which would logically have transfers of funds to brokerages or stock exchanges, payroll for employees, expenses for utilities, software, investment tools, etc. Rather, the only deposit activity present in the account is single transfer from V1. The only withdrawal activity are the subsequent transfers of 95.5 percent of the funds to **Subject Account 1** and the 4.5 percent of the funds that were sent to **Subject Account 2**.

26. The activity that "Carmona Inversiones" facilitated is consistent with the operation of a funnel account, a common money laundering technique that facilitates the rapid placement of illicit funds into the financial system from multiple geographical areas. The effect of moving the funds in this manner have the desired effect sought by criminal networks to move money rapidly while creating a complex audit trail that seeks to frustrate attempts by law enforcement and bank personnel to identify the origin of funds. As seen here, criminal networks will likewise use funnel accounts to skip the money through multiple different banks, so that the banking institutions involved only see fractional pieces of the entire transaction. In 2011, 2012, and 2014 the Financial Crimes Enforcement Network (FinCEN) issued advisories detailing the rise of funnel bank accounts as a technique employed by subjects seeking to move and launder illicit proceeds.[4] These advisories correspond with the manner in which the "Carmona Inversiones" bank account was used.

27. **Subject Account 2** also holds proceeds of laundering activity. Most notably, it received CARMONA's 4.5% commission for the $935,500 laundering effort. The entity "Bereshit Royalty LLC," the company associated with this account, is a Florida incorporated entity that was

[4] *See* FIN-2011-A009, FIN-2012-A006, and FIN-2014-A005.

established in November 2022. The FBI's research found a website for the entity (www.bereshitroyalty.com). The website was created to provide the appearance of legitimacy to fictitious businesses engaged in money laundering. Such fraud websites may include non-sensical or vague descriptions of the nature of the business; photographs and logos stolen from other websites; spelling and grammatical errors; and simple, templated designs. The website of "Bereshit Royalty" fits all these characteristics:

- *Appearance of the Website*: The website is quite basic and provides only generic business descriptions of Financial Advisory, Real Estate, and Cryptocurrency services that the business provides. The website shows purported photographs of CARMONA and "Gabriel Cavallini" as the Bereshit Royalty "team" and identify them both as "Financial Advisor – Real Estate." However, the photograph of CARMONA does not match his true appearance. Research of the headshot images used for both CARMONA and "Gabriel Cavallini" found the images to be those of models used in stock images that are found on dozens of websites. There are also icons contained below each photo for social media accounts for CARMONA and "Gabriel Cavallini," yet the links are not functional.
- *Nature of the Business*: The website explains that the business offers Financial Advisory, Real Estate, and Cryptocurrency services and gives vague information on these services. Links to "Discover Properties" that the business offers for sale/rent, and "Discover the Plans" for their financial advisory services, do not function. The website provides a basic explanation of cryptocurrency and states "Do you need more information or a capacitation on this subjet*[sic]*?" Of note, though "capacitation" sounds somewhat similar to the term "capital," it actually refers to the biochemical process in which sperm fertilizes an egg.
- *Location of the Business, United States*: The address provided for "Bereshit Royalty" is 8400 NW 36th Street, Doral, Florida – an office building that houses dozens of businesses on site. A search of the building's online directory was negative for

"Bereshit Royalty." The fact that there is no suite number specified for the business in this multi-office facility is consistent with the business being non-existent. Open-source searches for business listings did not turn up any indications of the existence of "Bereshit Royalty" in Doral, Florida or elsewhere. The phone numbers listed for the business are Costa Rica phone numbers.

28. "Rogas Management LLC" has no internet presence outside of its incorporation documents and the business address returns to an office that formerly belonged to the attorney who registered the entity.

Additional Subjects Accounts / Fraud Victim – V2

29. In May 2024, the CHS reported that S1 continued to process funds related to the fraud scheme. On or about May 24, 2024, S1 directed the deposit of a $70,000 check to **Subject Account 1** and asked the accountholder to provide an equivalent amount of funds in USDT cryptocurrency. The $70,000 check was issued from a Community America Credit Union account for V2. This transaction did not go through, and the funds were returned to V2's account.

30. On May 29, 2024, the FBI contacted V2. V2 is an elderly resident of Missouri and a retired school superintendent. V2 explained that V2 sent the $70,000 at the direction of subjects who contacted V2 about winning a large amount in a sweepstakes contest starting approximately one year ago. V2 admitted to sending over $1 million dollars to date at the direction of these subjects – sending the funds via check deposit and at times via cashier's checks that V1 mailed to addresses in Myrtle Beach, South Carolina. The subjects instructed V2 to send these funds, which they explained were taxes and fees that were required to be paid before V2 could collect the sweepstakes winnings. The subjects who called V2 claimed to be bank employees, attorneys, and other officials to include Supreme Court Justice Neil Gorsuch. The $70,000 check that V2

deposited to **Subject Account 1** was the latest installment in taxes and fees that V2 was directed to pay by these subjects.

31. At the time of the call, V2 confirmed that V2 had received the $70,000 that had been refunded by **Subject Account 1**. The FBI warned V2 that he/she would be likely contacted by the fraudsters shortly, to direct V2 to re-deposit the funds to another bank account in an attempt to continue to defraud V2.

32. On May 30 and June 4, 2024, V2 contacted the FBI and reported that the fraudsters had made contact and explained that the reason the $70,000 check was refunded was because V2 had sent this check to the "wrong department." The fraudsters sent V2 instructions to send the funds to two new accounts, one of which was **Subject Account 3.** The fraudsters continued to call V2 daily, and aggressively pressure V2 to deposit his/her money to the accounts immediately.

33. V2 reviewed bank statements and identified previous instances in which V2 sent funds to the fraudsters and provided bank records corroborating some of the transfers. For others, which V2 could not locate bank records, the FBI have confirmed the transactions with bank records provided by the respective financial institutions. This review has revealed the following:

- Between December 2022 and July 2023, V2 sent checks and wires transfers to **the** fraudster's accounts.
- On February 23, 2023, V2 was instructed by the fraudsters to obtain a cashier's check for $43,890 payable to "Digital Silverback LLP." V2 was then instructed to mail the check to "Hugo Solano" at 307 75 Ave N, Myrtle Beach, South Carolina.
- On March 6, 2023, V2 was instructed by the fraudsters to send $35,529 to "Digital Silverback LLP" account held at Novo Bank account 101067967 via wire transfer. Incident to this transfer, the fraudsters instructed V2 to state that the purpose of the wire was for the "purchase of property."
- On March 22, 2023, V2 was instructed to obtain a cashier's check for $40,000 payable to "Digital Silverback." V2 was then instructed to mail the check to "Hugo Solano" at 307 75 Ave N, Myrtle Beach, South Carolina.

- On March 21, 2023, V2 was instructed by the fraudsters to obtain a $42,000 cashier's check payable to "Digital Design and Graphic Solutions LLP." V2 was then instructed to mail the check to "Hugo Solano" at 307 75 Ave N, Myrtle Beach, South Carolina.

"Digital Design and Graphics Solutions LLP" and "Digital Silverback LLP"

34. "Digital Design and Graphics Solutions LLP," the purported entity associated with **Subject Account 3**, was incorporated in South Carolina on October 11, 2024. Similarly, "Digital Silverback LLP," was incorporated on May 11, 2020, in South Carolina. Both entities were incorporated by Hugo Francisco Solano (HUGO).

35. Both entities purport, in paperwork prepared on their behalf, to be "digital and technical programming and design" companies. The address for both businesses is 307 75th Ave N, Myrtle Beach, South Carolina; open-source research shows that this is a two-bedroom residential home in a suburban neighborhood. There is no physical signage present at the address, and no evidence (per a check of business-listing services) of a business being operated there. Despite the businesses purporting to be engaged in digital design and programming, open-source searches found no websites, customer reviews, or evidence of the existence of these businesses.

36. HUGO is the sole person named in the incorporation documents for both entities, yet he is not listed as the signatory on any of the relevant **Subject Accounts**. Rather, **Subject Account 3** was opened by Savannah Solano (SAVANNAH) – an apparent family member – and another bank account was opened by Lamara Leachman (LEACHMAN), a current or former spouse of HUGO. SAVANNAH and LEACHMAN were identified as 25% owners of "Digital Design and Graphics Solutions LLP," and LEACHMAN as a 25% owner of "Digital Silverback LLP."

37. Records checks show that HUGO is a Costa Rican national who was arrested in New York on June 10, 2008, for impersonating a United States citizen to acquire a firearm. Following

this incident, HUGO was arrested by ICE in June 2009 as a deportable alien and deported to Costa Rica on or about March 2, 2011. From our investigation, we believe he is currently living in Myrtle Beach, South Carolina. Customs and Border Protection has run preliminary records checks on HUGO, which shows his conviction and removal, but did not show that he has permission to enter the United States, a visa, or a work authorization. HUGO is likely residing in the United States illegally, without authorization to work here.

38. Additionally, investigators have received information tending to corroborate the view that HUGO is using accounts unlawfully. Another FBI Office investigated HUGO several years ago in a money-laundering and drug-trafficking investigation. That investigation also focused on HUGO using domestic bank accounts to receive illicit funds linked to illicit offshore gambling. As part of that investigation, another CHS reported that in 2021, HUGO was using a bank account for "Digital Silverback LLP" to receive and launder gambling proceeds.[5] The CHS provided communications and documents to support this reporting.

39. The information about HUGO's apparent use of accounts for illicit gambling is consistent with contemporaneous information the FBI has gathered. On June 4, 2024, investigators identified a phone number for another individual, V5, who had sent repeated wire transfers totaling $127,500 to **Subject Account 3** and contacted V5 via telephone. We asked V5 about the wire transfers V5 had sent to **Subject Account 3**. V5 confirmed that V5 had sent over $100,000 to the account and confirmed the following transactions in 2024: May 6, for $25,000; May 13, for $45,000; May 21, for $38,500; and June 3, for $19,000.

[5] The CHS-3 was recruited in early 2021 after being arrested for a bulk-cash offense. The CHS agreed to cooperate in the hopes of receiving consideration on possible charges. No promises were made to the CHS in this regard. The CHS provided information that the FBI corroborated with stored communications, bank documents, and consensually recorded communications. The CHS provided information that led to currency and weapons seizures, and identification of targets of investigation. In late 2023, the FBI deactivated the CHS for cause, when the CHS committed an unauthorized act that may have been illegal in and of itself, but which appeared at least to facilitate other illegal activity.

40. V5 stated the funds were sent at the direction of representatives of a Costa Rica-based online gambling platform, "www.betonsports.online." After sending the funds, V5 was provided an equivalent amount of funds (or virtual "chips") used to play blackjack via the online website.

41. Account activity for Subject Account 3 in the name of "Digital Design and Graphics," consisted of receiving ACH wire transfers, check deposits, and cashier's check deposits from third party individuals. Upon receiving the funds, the account holder transferred large amounts of money to other accounts. The account had no payments consistent with the operation of a digital and graphic design/programming company, such as payroll, utilities, hardware and software purchases or subscription fees, rental of an office facility, etc. The primary source of funds over the last several weeks prior to seizure were check deposits from V5 and an entity, that appears from its name to be related to the family of V5, referenced to as V6. Since the beginning of May 2024, **Subject Account 3** had received four wire transfers totaling $127,500 from these entities.

Investigation Identifies Multiple Fraud Victims Who Have Sent Funds to "Digital Silverback LLP" and "Digital Designs and Graphics LLP"

42. In addition to the victims discussed thus far, a search of law enforcement databases has identified additional victims who have been directed by fraudsters to send money to "Digital Silverback LLP" and "Digital Designs and Graphics LLP." These findings support the FBI's conclusion that the identified "programming and design" businesses do not exist and are fronts for the Costa Rica-based fraud and money laundering organization. We note the following:

- On June 5, 2024, the FBI contacted Trustmark National Bank to inquire about a fraud incident involving "Digital Silverback LLP" and "Digital Design Marketing LLP." A bank representative reported that in February 2023, the bank was contacted by the child of an accountholder, whom the bank representative reported was falling victim to scams. Trustmark Bank's investigation found that the accountholder was acting as an unwitting money mule, repeatedly receiving funds from V11 in Arizona and transferring funds to a bank account for "Digital Silverback LLP." Trustmark Bank

learned that V11 had believed they had won the "Publisher's Clearing House" and the funds being sent were fees that had to be paid before V11 could receive the prize.

- V12, an elder resident of California was interviewed by the FBI on July 9, 2019. V12 was contacted by fraudsters claiming she had won a Publishers Clearing House prize. V12 sent numerous payments at the direction of the fraudsters in excess of $100,000. After refusing to pay more money, V12 was asked to receive packages of money and checks at her residence (*i.e.*, V12 was recruited as a money mule). At the fraudster's directions, V12 deposited the cash, checks, and money orders in bank accounts that V12 opened, and wired funds to unknown persons in Costa Rica. Incident to these transfers, the fraudsters instructed V12 to provide a cover story to bank personnel for the transfers that V12 was building a home in Costa Rica. Despite being provided a "money mule letter" and being advised by the FBI that V12 was laundering money, V12's work for the fraudsters appears to have continued. In November 2023, V12 deposited two USPS money orders totaling $2,000 to an account.
- V13, a resident of Ohio, reported to the FBI on March 9, 2022, that V13 was targeted by fraudsters who convinced V13 that they had won a cash prize from "Good Housekeeping." V13 sent a total of $24,874 in money orders, checks, and wires to several entities, including "Digital Silverback LLP" in Myrtle Beach, South Carolina at the direction of the fraudsters.
- V14's child reported to the FBI on February 10, 2023, that V14's parent was being targeted by fraudsters, who had told V14 that V14 had won millions of dollars. The fraudsters directed V14 to send four personal checks to the Trustmark Bank accountholder who also unwittingly moved V11's money. V14 tried to purchase a $20,000 cashier's check payable to "Digital Silverback" but was stopped when bank employees intervened.
- A friend of V15 reported to the FBI on June 29, 2022, that V15 was being targeted by fraudsters who told V15 that they had won a lottery and needed to send funds

before V15 could collect the winnings. The fraudsters convinced V15 to sell a vehicle to raise the funds. After sending an initial series of money orders, V15 was targeted a second time, this time the fraudsters claimed they were an attorney who could sue the fraudsters. V15 sent $37,000 to a Bank of America account for "Digital Silverback LLP." (This account has since been closed by Bank of America.)

Interview of Hugo SOLANO

43. Following the seizure of **Subject Account 3**, the FBI conducted recorded interviews with both Hugo SOLANO ("HUGO") and his daughter Savannah. Savannah explained that she opened and operated **Subject Account 3** at the direction of her father HUGO. Unknown persons mailed checks to Savannah's address, and she would subsequently deposit the checks into **Subject Account 3**.

44. The FBI also interviewed HUGO. HUGO was deported from the United States approximately 10 years before the interview and owned a restaurant in Costa Rica. In Costa Rica, he was approached by unknown persons who asked him to open bank accounts to receive money in the United States. These persons had learned that HUGO spoke English and sounded "American." HUGO agreed and setup a number of bank accounts to include **Subject Account 3.**

45. HUGO enlisted the help of his ex-wife and daughter to establish the accounts and receive money in the United States. The operation worked as follows:

- (1) HUGO received a phone call from unknown persons to advise him that a check of a designated amount was being mailed to his daughter's address (or) that funds were going to be sent to one of his accounts via wire transfer.

- (2) The checks were deposited by HUGO's daughter or ex-wife into the accounts. The funds were then wired to bank accounts in Costa Rica that HUGO controlled.
- (3) HUGO withdrew the money in cash from the Costa Rican accounts. HUGO gathered the money which would be intermittently collected by an unknown male on a motorcycle who picked up the cash from HUGO. HUGO collected a 3% commission on the funds he moved in this manner.

46. HUGO did not know the source of the money he was transacting. At the latter end of the call HUGO admitted that he believed the money was from offshore gambling and sportsbooks operations.

47. Based on the information and allegations set forth herein, there is a factual basis to support a reasonable belief that the Government will be able to meet its burden of proof at trial to show that the Defendant Funds constitutes, or is traceable to:

a. property involved in wire fraud transactions, attempted wire fraud transactions, or conspiracy thereof in violation of 18 U.S.C. §§ 1343, 1349;

b. property involved in money laundering transactions or attempted transactions in violation of 18 U.S.C. § 1956(a)(1)(A)(i), and/or § 1956(a)(1)(B)(i), and/or § 1956(a)(2);

c. property involved in an illegal money transmitting business, in violation of 18 U.S.C. § 1960; and/or

d. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(c)(7);

e. proceeds of some other form of specified illegal activity set forth in 18 U.S.C. § 1956(h); and

f. property involved in money transactions in criminally derived property, in violation of 18 U.S.C. § 1957.

CONCLUSION

48. By reason of these premises, and pursuant to 18 U.S.C. § 981(f) and 21 U.S.C. § 881(h), whereby the Plaintiff's right, title and interest in and to the Defendant Funds relates back to the commission of the act giving rise to the forfeiture, the Defendant Funds has become and is forfeited to the United States of America, to be disposed of pursuant to Supplemental Rule G(7)(c) for Admiralty or Maritime Claims and Asset Forfeiture Actions, 18 U.S.C. § 981(d), 21 U.S.C. § 881(e), and other applicable laws.

WHEREFORE, Plaintiff prays that due process issue to enforce the forfeiture of the Defendant Funds, *in rem*; that a Warrant for the Arrest of the Defendant Funds be issued; that due Notice be given to all interested persons to appear, make claim, answer and show cause why the forfeiture should not be decreed; that the Defendant Funds be decreed condemned and forfeited to the United States of America for disposition according to law; and that Plaintiff have such other and further relief as the Court may deem just and proper, together with the costs and disbursements of this action.

[SIGNATURE PAGE TO FOLLOW]

Respectfully submitted,

Adair F. Boroughs
UNITED STATES ATTORNEY

By: *s/Carrie Fisher Sherard*
Carrie Fisher Sherard #10134
Assistant United States Attorney
55 Beattie Place, Suite 700
Greenville, SC 29601
(864) 282-2100

October 10, 2024